UNITED STATES PATENT AND TRADEMARK OFFICE   m n

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/651,548	08/29/2000	Barry Atkins	RPS920000026US1	9903

42640   7590   07/11/2007

DILLON & YUDELL LLP
8911 NORTH CAPITAL OF TEXAS HWY
SUITE 2110
AUSTIN, TX 78759

EXAMINER
SHIN, KYUNG H

ART UNIT	PAPER NUMBER
2143	

MAIL DATE	DELIVERY MODE
07/11/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>05 April 2007</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-24</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-24</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

PROSECUTION REOPENED

1. In view of the Appeal Brief filed on 4/11/2005, PROSECUTION IS HEREBY

REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the

following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply

under 37 CFR 1.113 (if this Office action is final); or,

(2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied

by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130,

1.131 or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

2. This action is responding to BPAI Decision filed 4/5/2007. Claims **1 - 24** are

pending. Independent claims are **1, 9, 17**.

Claim Rejection – 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4.   **Claims 1 - 4, 6 - 12, 14 - 20, 22 - 24** are rejected under 35 U.S.C. 103(a) as being

unpatentable over **Doonan et al.** (US Patent No. **6,807,277**) in view of **Cook** (US

Patent No. **6,732,101**).

Regarding Claims 1, 9, 17, Doonan discloses a network messaging system. (see

Doonan col. 1, lines 10-12: " *... present invention is directed to a secure electronic*

messaging system ... ") Doonan discloses a method, a system and program product for

managing a user key used to sign a message for a data processing system, the method

comprising:

   a) assigning a user key to a user and storing the user key in <u>an encrypted</u> data

      processing system <u>utilized to</u> encrypt messages; (see Doonan col. 2, lines 1-7:

      encryption key assigned by key server for message encryption)

   b) encrypting the messages with the user key; (see Doonan col. 2, lines 7-8:

      message is encrypted)

   c) storing an associated key in the <u>encrypting</u> data processing system and encrypting

      the user key with the associated key to obtain an encrypted user key; (see Doonan

      col. 5, lines 63-67: generate an encrypted user key for transmission)

   d) <u>the encrypting data processing system</u> communicating <u>at least one</u> encrypted

      messages <u>together</u> with the encrypted user key <u>to a recipient system in order</u> to

      <u>permit validation of</u> an association of the user with the encrypted messages <u>by the</u>

      <u>recipient system</u>; (see Doonan col. 6, line 1: encrypted message and encrypted

      key are transmitted to recipient)

f) computer usable media bearing the control program. (see Doonan col. 3, lines 9-

12; col. 9, lines 33-44: software exists on computer readable medium for program

execution)

Doonan discloses a check on the validation of a sender's credentials. (see

Doonan col. 5, lines 16-20: sender credentials are verified)   Doonan does not

specifically disclose revoking the associated key <u>at the encrypting data processing</u>

<u>system</u> to prevent validation.

However, Cook discloses:

e) preventing validation of the association of the user with messages by revoking

the associated key <u>at the encrypting data processing system</u> (see Cook col. 6,

lines 40-50: association key deleted (revoked: see spec. page 15 lines 27-28

"Associated key A may be **revoked by simply erasing it** from server system

104.") as per specification by software component at the user system software

component residing (data encryption system))

It would have been obvious to one of ordinary skill in the art at the time the

invention was made to modify Doonan to delete (revoke) an association key and

prevent validation of the association of the user as taught by Cook. One of ordinary

skill in the art would be motivated to employ Cook in order to enable a flexible and

strengthened encryption system. (see Cook col. 2, lines 33-38: " ... *Messages can be*

encrypted using any available encryption means at the sender and sent to a

forwarding service. The forwarding service can forward the message to each recipient

according to the recipient's decryption capability and preference. ... ")

Regarding Claims 2, 10, 18, Doonan discloses the method, system and program

product according to Claims 1, 9, 17, further comprising:

a) decrypting the user key with the associated key; (see Doonan col. 6, lines 1-3:

encrypted key is decrypted)

b) decrypting the messages with the user key. (see Doonan col. 6, lines 1-3:

encrypted message is decrypted)

Regarding Claims 3, 11, 19, Doonan discloses the method, system and program

product according to Claims 1, 9, 17, wherein: the <u>encrypting</u> data processing system

further comprises a client system <u>and a server system coupled for communication, the</u>

<u>client system</u> (see Doonan col. 3, lines 9-12: network connected client (sender) and

server system) having a client memory device <u>and the</u> server system having an

encryption chip and a server memory device:

a) storing the user key further comprises storing the user key in the client memory

device; (see Doonan col. 9, lines 44-47: memory area used for data and

workspace storage)

b) storing the associated key further comprises storing the associated key in the

server memory device; (see Doonan col. 5, lines 4-5: key is stored at server

system database)

Doonan discloses a check on the validation of a sender's credentials. (see Doonan col. 5, lines 16-20: sender credentials are verified)   Doonan does not specifically disclose preventing validation of messages associated with the user by eliminating the associated key from the server memory device.

However, Cook discloses:

c) preventing validation further comprises preventing validation of messages associated with the user by eliminating the associated key from the server memory device. (see Cook col. 6, lines 40-50: deletion (revocation) of association key at system via software component on server system in order to prevent validation)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Doonan to prevent validation of messages associated with the user by eliminating the associated key as taught by Cook. One of ordinary skill in the art would be motivated to employ Cook in order to enable a flexible and strengthened encryption system. (see Cook col. 2, lines 33-38)

Regarding Claims 4, 12, 20, Doonan does not disclose a server system to receive, encryption and forward message. However, Cook discloses the method, system and program product according to Claims 3, 11, 19, wherein encrypting the messages further comprises:

a) sending the messages to be encrypted from the client system to the server

   system; (see Cook col. 2, lines 19-23: send message from client to server for

   encryption)

b) encrypting the messages using the encryption chip of the server system; (see

   Cook col. 2, lines 51-55: encrypt message)

c) sending the encrypted messages from the server system to the client system. (see

   Cook col. 2, lines 51-55: deliver encrypted message to recipient (client) system)

   It would have been obvious to one of ordinary skill in the art at the time the

invention was made to modify Doonan to send messages, encrypt messages, and

retrieve encrypted messages as taught by Cook. One of ordinary skill in the art would

be motivated to employ Cook in order to enable a flexible and strengthened encryption

system. (see Cook col. 2, lines 33-38)

Regarding Claims 6, 14, 22, Doonan discloses the method, system and program

product according to Claims 1, 9, 17, further comprising: encrypting the associated key

by using an encryption chip key which is stored on an encryption chip of the encrypting

data processing system. (see Doonan col. 2, lines 3-8: encryption key transferred to

sender system)

Regarding Claims 7, 15, 23, Doonan discloses the method, system and program

product according to Claims 6, 14, 22, further comprising:

communicating an encrypted associated key to validate the association of the user with

the encrypted messages. (see Doonan col. 5, lines 63-67:)

Regarding Claims 8, 16, 24, Doonan discloses the method, system and program product according to Claims 7, 15, 23, further comprising: decrypting the associated key with the encryption chip key. (see Doonan col. 6, lines 1-3)

5.   **Claims 5, 13, 21** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Doonan-Cook** and further in view of **Marshall** (US Patent No. **4,888,800**).

Regarding Claims 5, 13, 21, Doonan-Cook does not disclose the ability to erase key information after processing of an encrypt message. However, Marshall discloses the method, system and program product according to Claims 4, 12, 20, further comprising: erasing from the server system all data relating to the encrypted messages after the encrypted messages are sent from the server system to the client system. (see Marshall col. 2, lines 30-35: key information is erased from system)

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Doonan-Cook to erase all key related information after message processing maintaining only current information as taught by Marshall. One of ordinary skill in the art would be motivated to employ Marshall in order to enable a flexible and strengthened network key management system. (see Marshall col. 1, lines 50-58: " ... *system has the advantage ... only to maintain the keys required for whatever current communication sessions ... a pair of session keys ... every time a link or session is requested ...* ")

Conclusion

6.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Kyung H. Shin whose telephone number is (571) 272-

3920. The examiner can normally be reached on 9:30 am - 6 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, David A. Wiley can be reached on (571) 272-3923. The fax phone number

for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

K H S
Kyung Hye Shin
Patent Examiner
Art Unit 2143

KHS
June 25, 2007

DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100